Carnegie Mellon University

Copyright 2015 Carnegie Mellon University

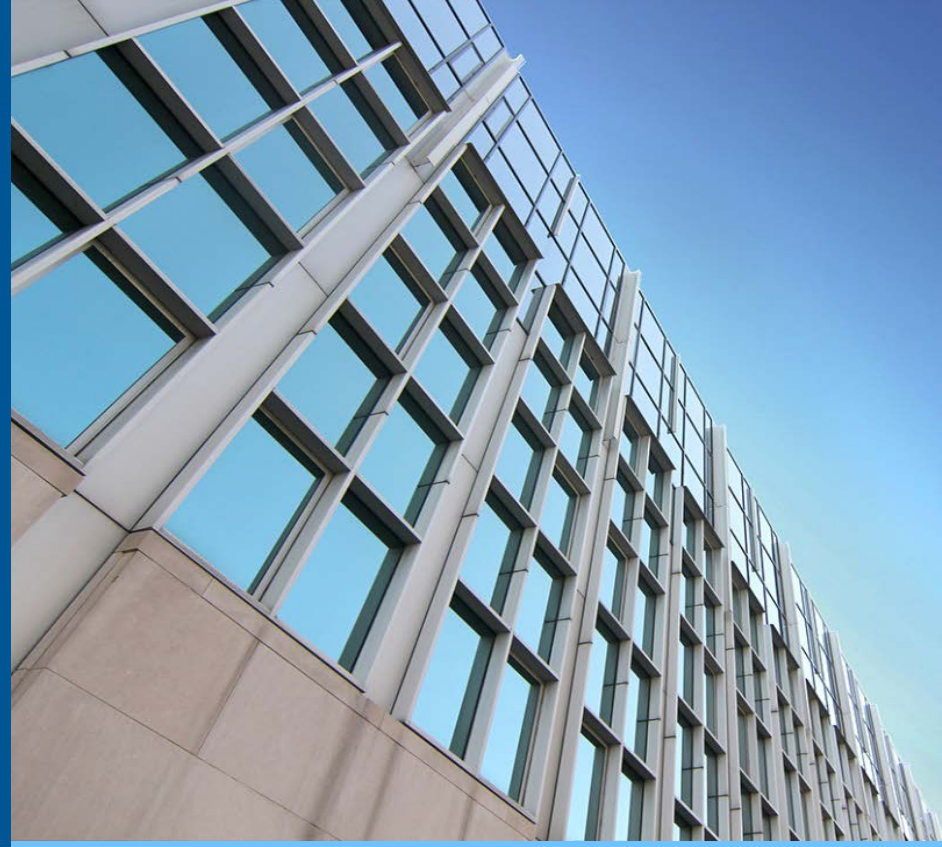
This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM-0003080

Using Network Flow to Gain Cyber Situational Awareness

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Sidney Faber



Polling Question 1

How familiar are you with the concept of “Cyber Situational Awareness”?

- Sounds interesting, but I haven’t put much thought into it
- I’m familiar with situational awareness, but have never applied it to cyber
- It’s an important part of my work but I would like to better understand it
- I’ve studied and applied the concept extensively

Polling Question 2

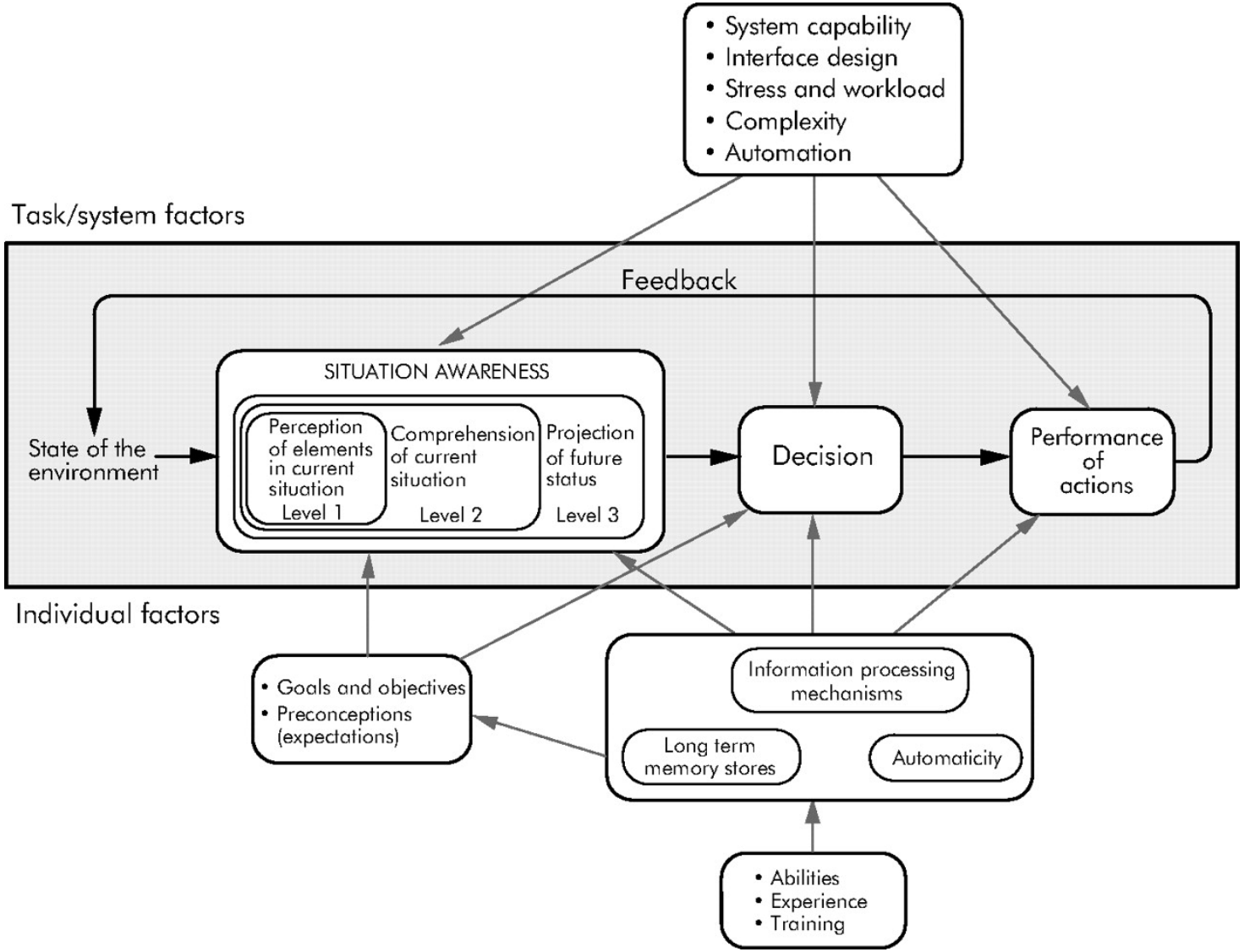
What is your background?

- Executive management
- Technical management
- Operational leader (e.g., shift supervisor)
- Technical or operational staff

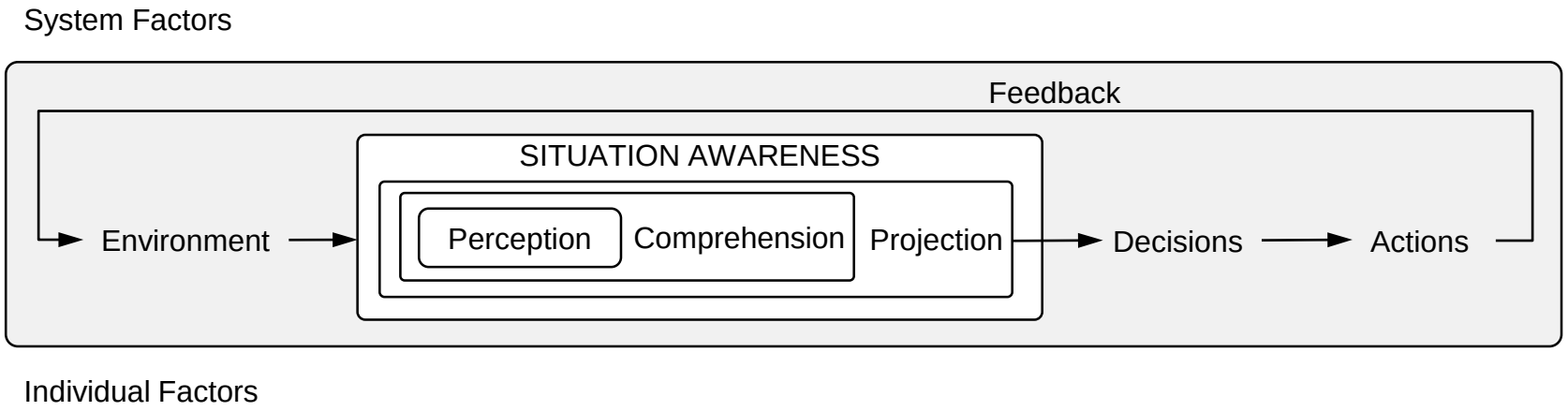
Situation Awareness Is a State of Knowledge

Situation awareness is the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future.

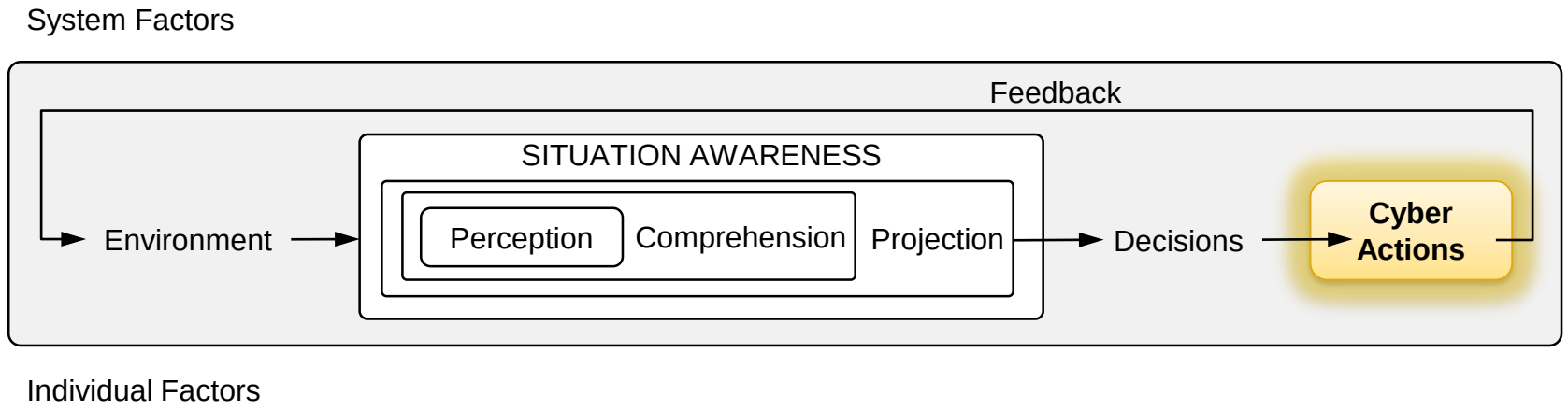
Endsley, M. R. SAGAT: A methodology for the measurement of situation awareness (NOR DOC 87-83). Hawthorne, CA: Northrop Corp.



Endsley, M. R. *Toward a Theory of Situation Awareness in Dynamic Systems*. Human Factors, 1995, 37(1), 32-64

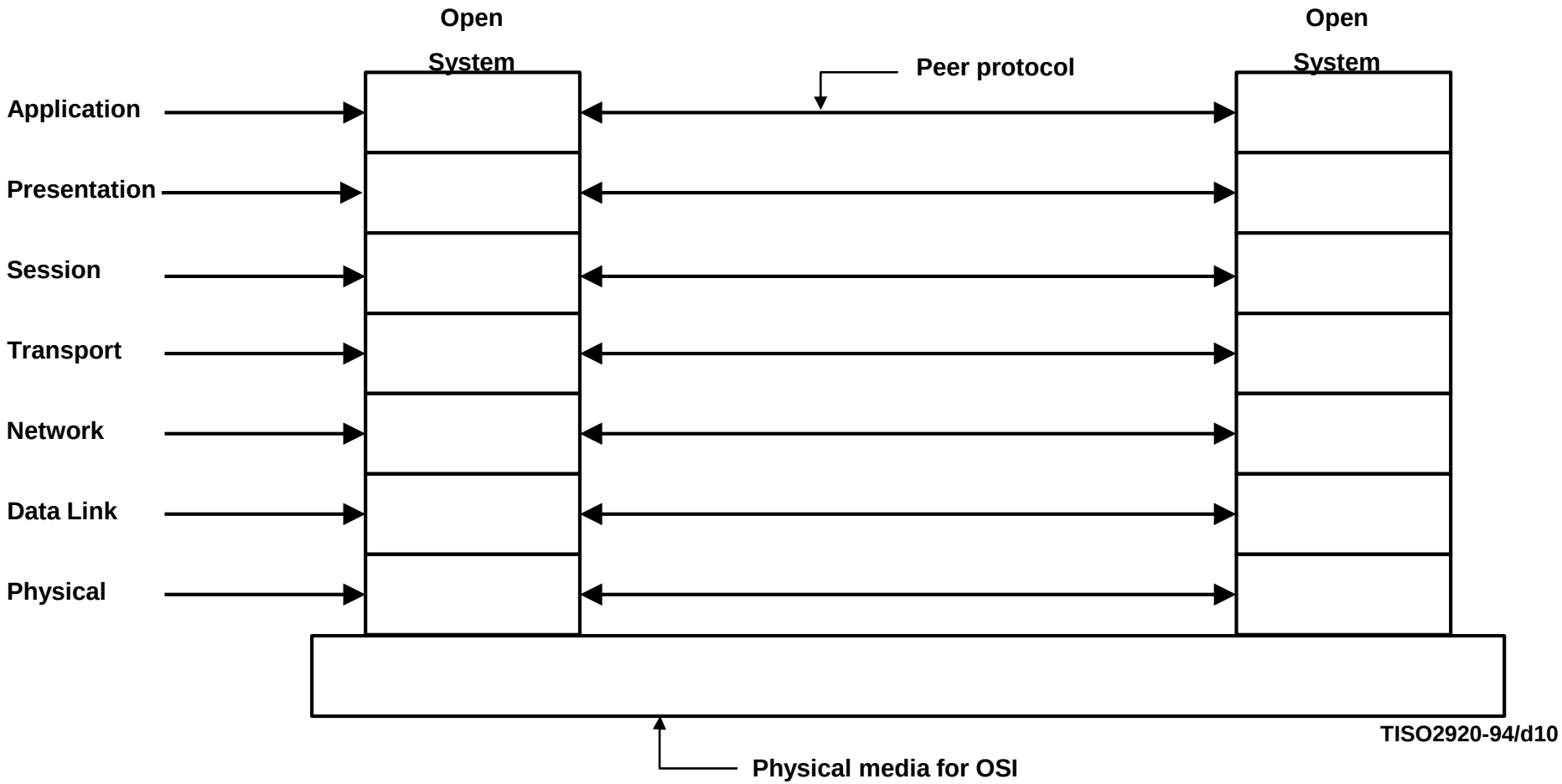


Situation awareness is the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future.



Cyber situational awareness is the subset of all situation awareness necessary to support taking actions in cyber.

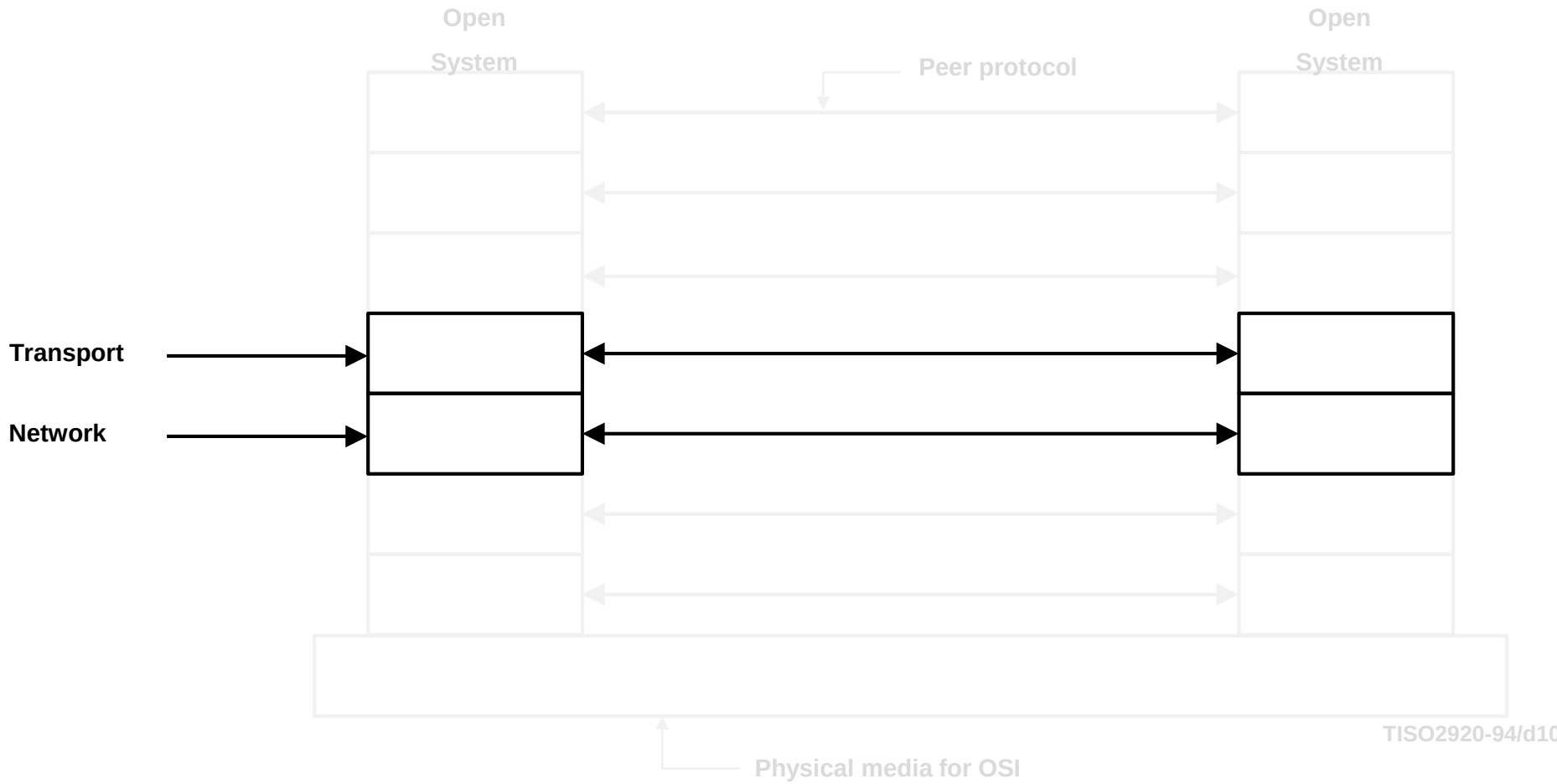
The Open System Model



ISO 7498 para 6.1.3 page 28

Figure 11 – Seven layer reference model and peer protocols

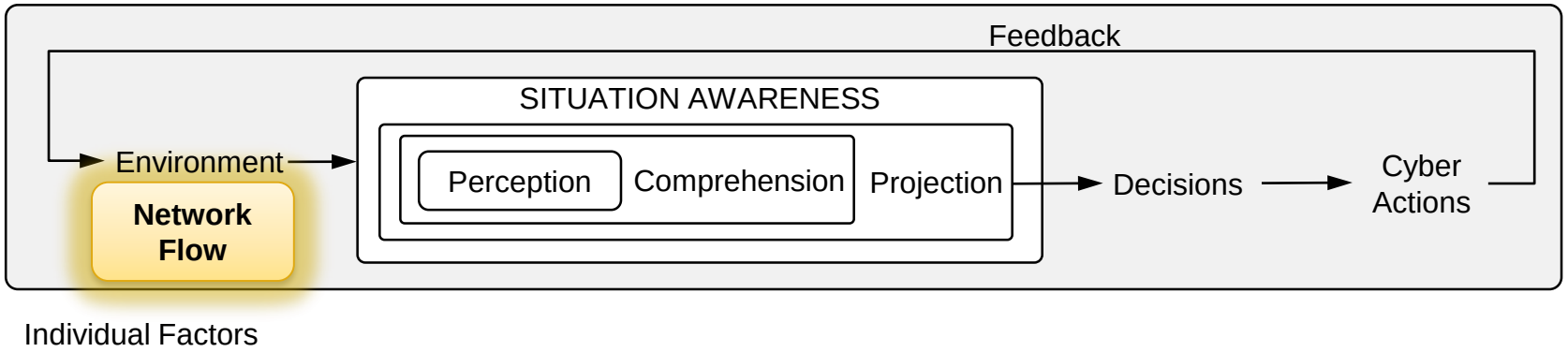
The Open System Model



ISO 7498 para 6.1.3 page 28
Figure 11 – Seven layer reference model and peer protocols

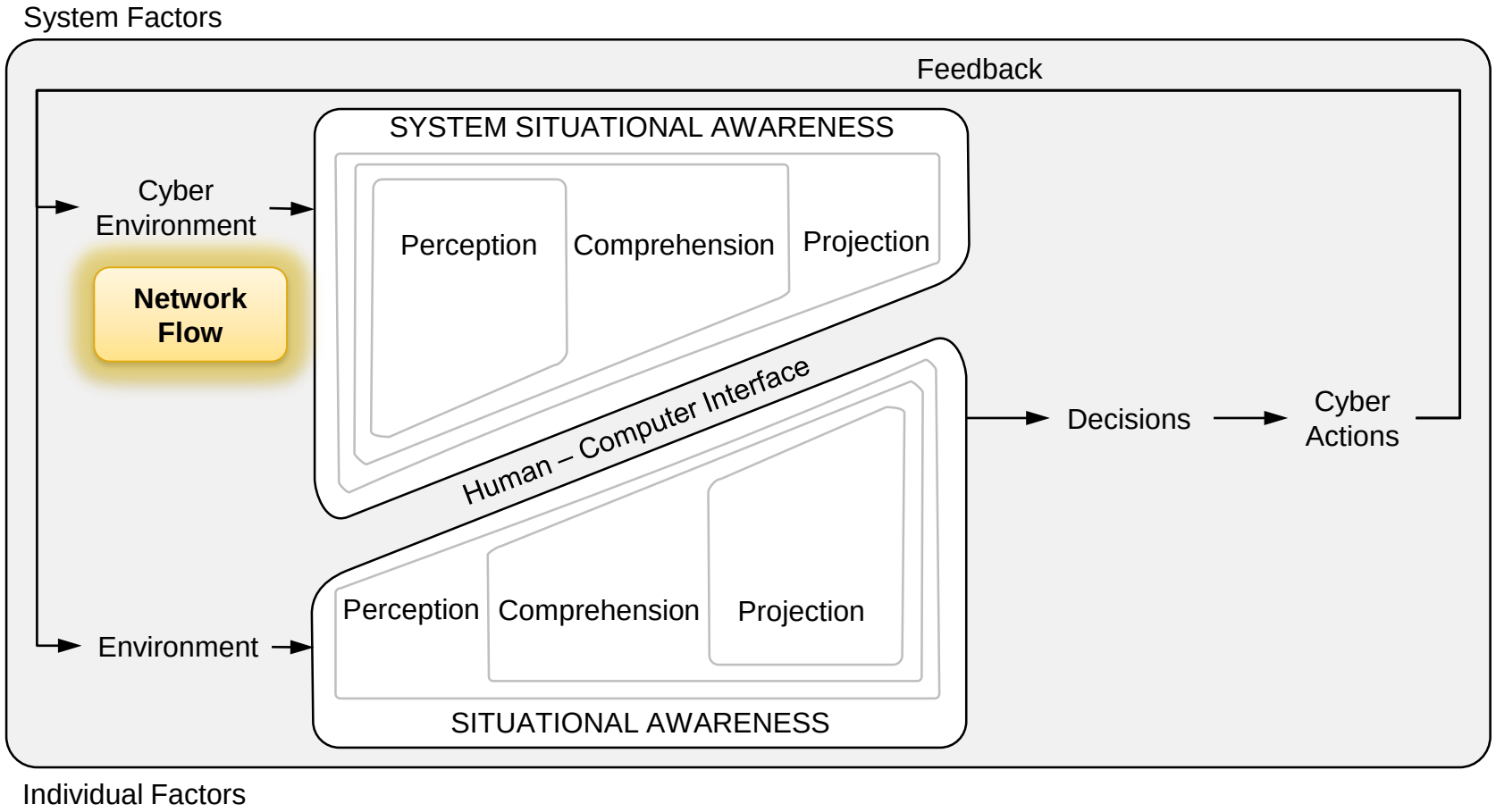
Environment

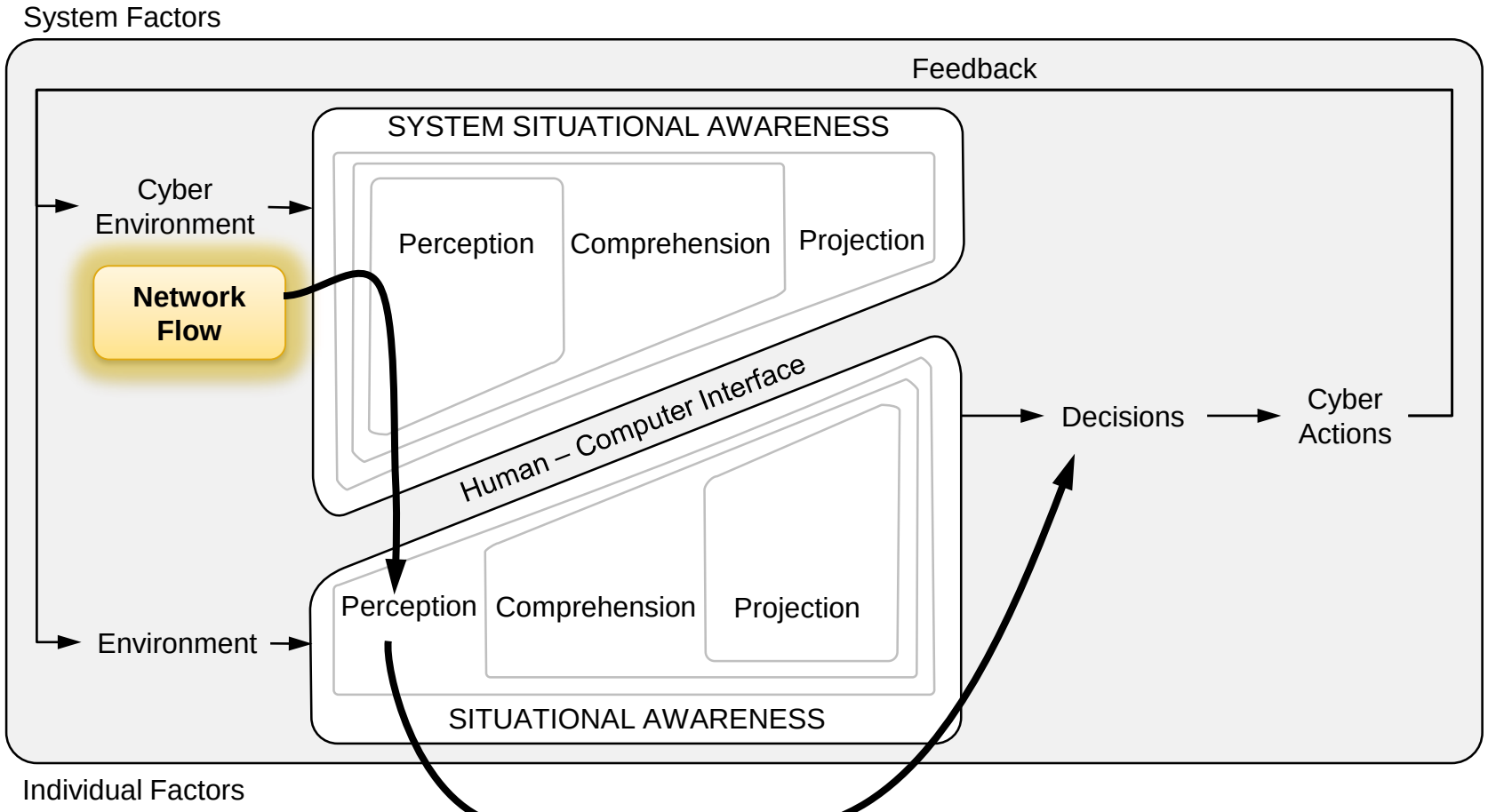
System Factors



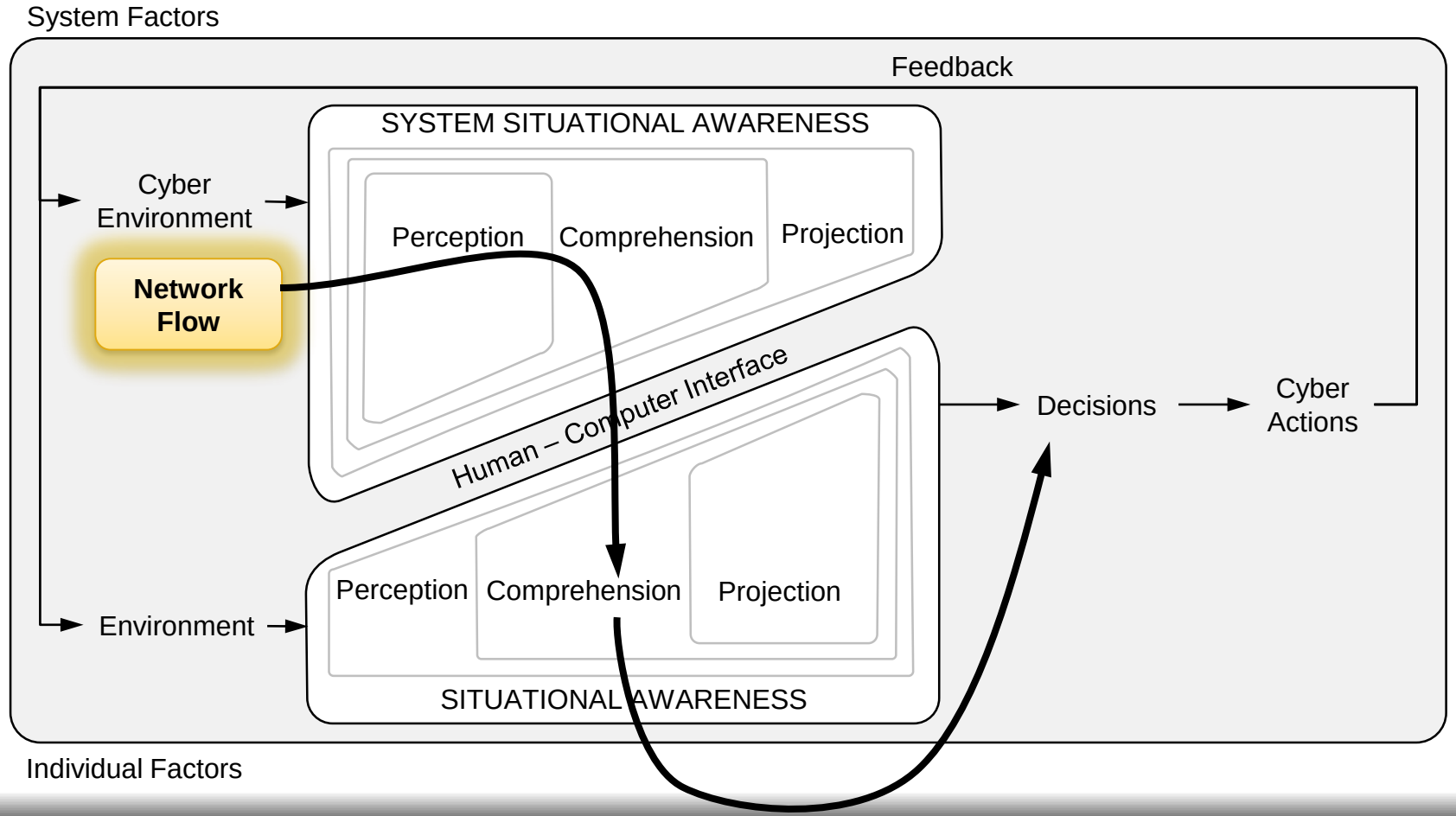
Individual Factors

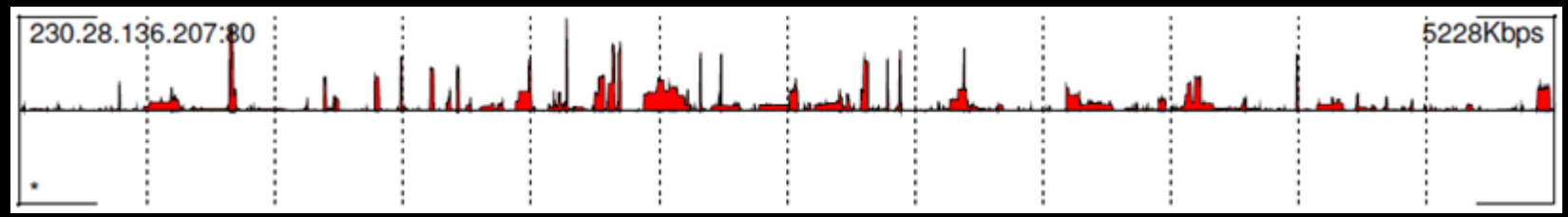
Cyber situational awareness is the subset of all situation awareness necessary to support taking actions in cyber.

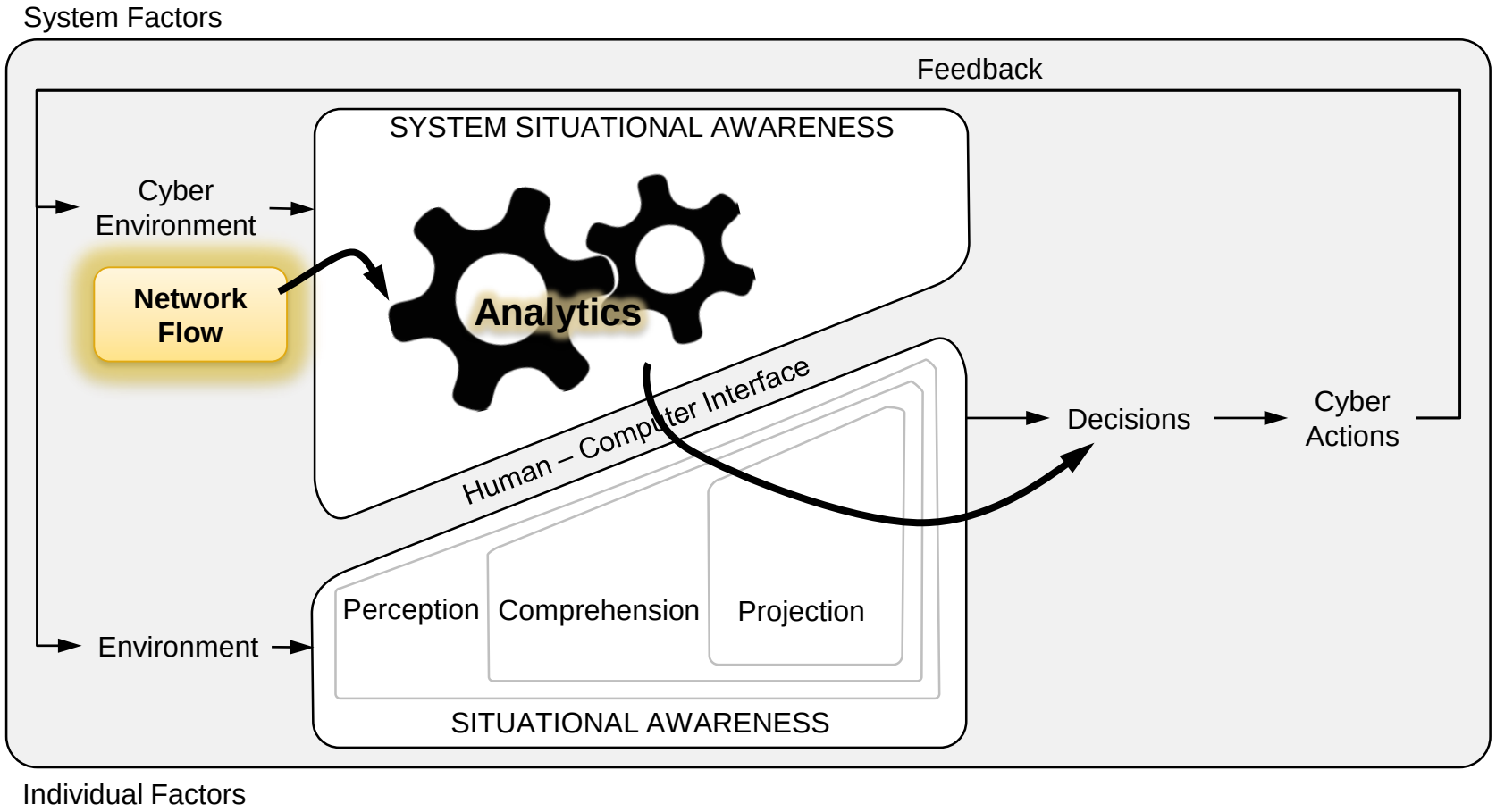


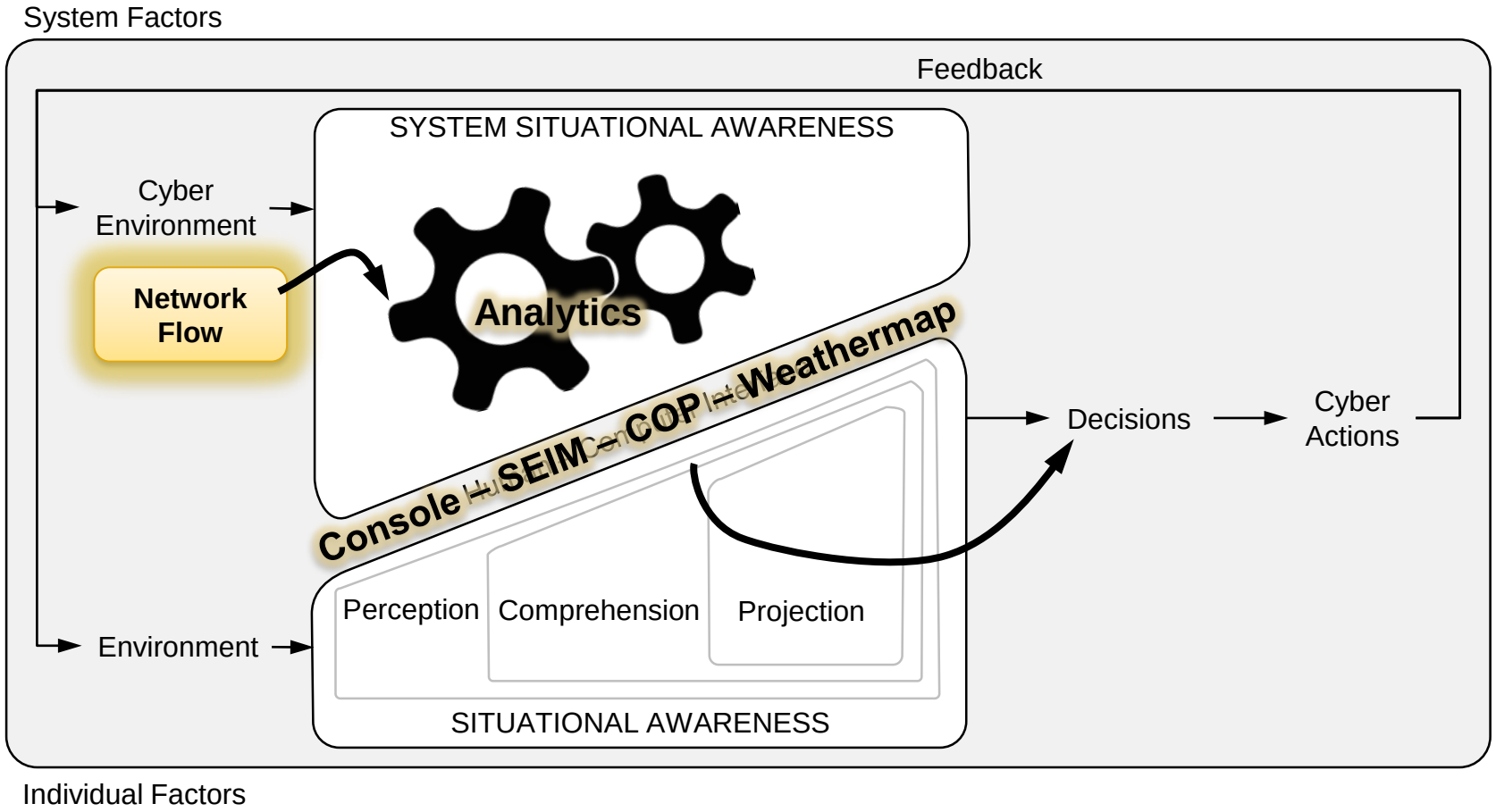


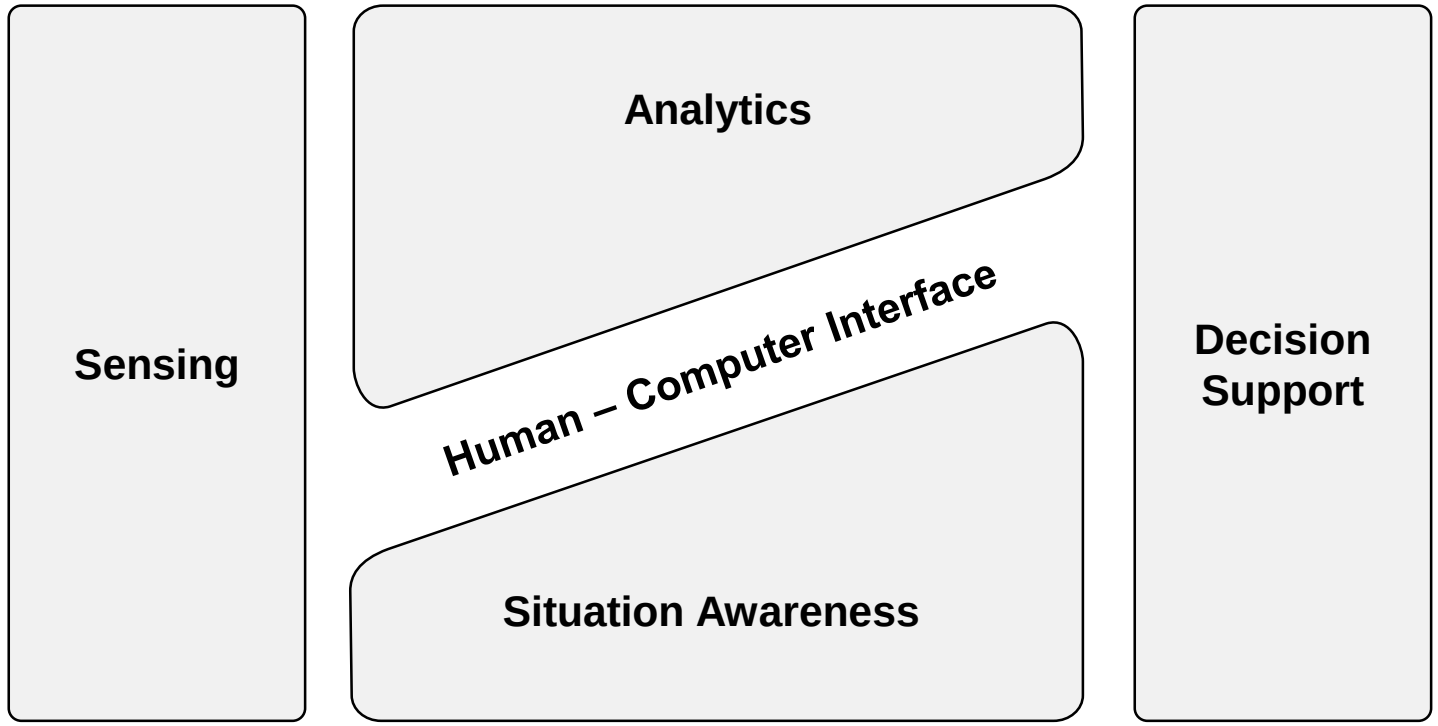

```
          sIP|          dIP|sPort|dPort|pro|packets|flags|initF|  type|
192.168.1.105| 198.51.100.6|49152|   80|  6|      4| SRPA| S   |outweb|
 198.51.100.6|192.168.1.105|   80|49152|  6|      3| S PA| S  A| inweb|
```





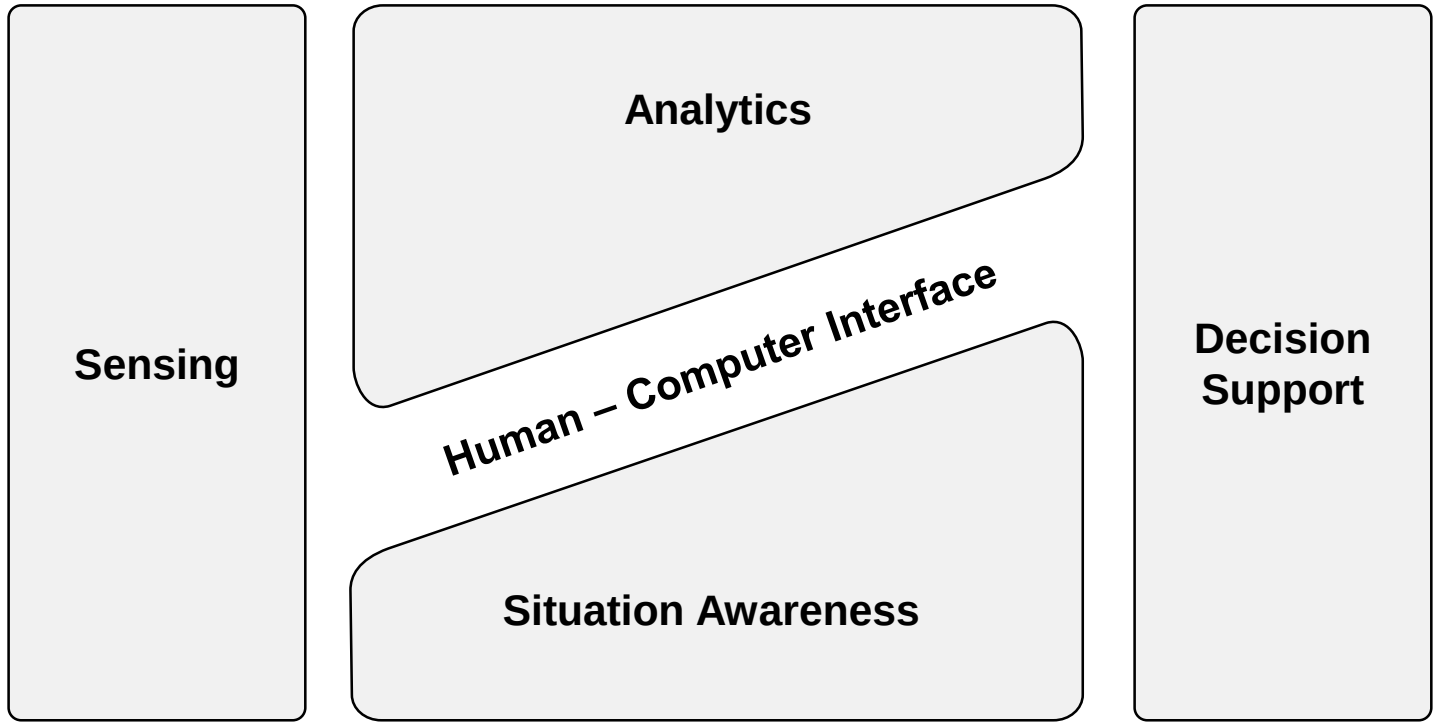


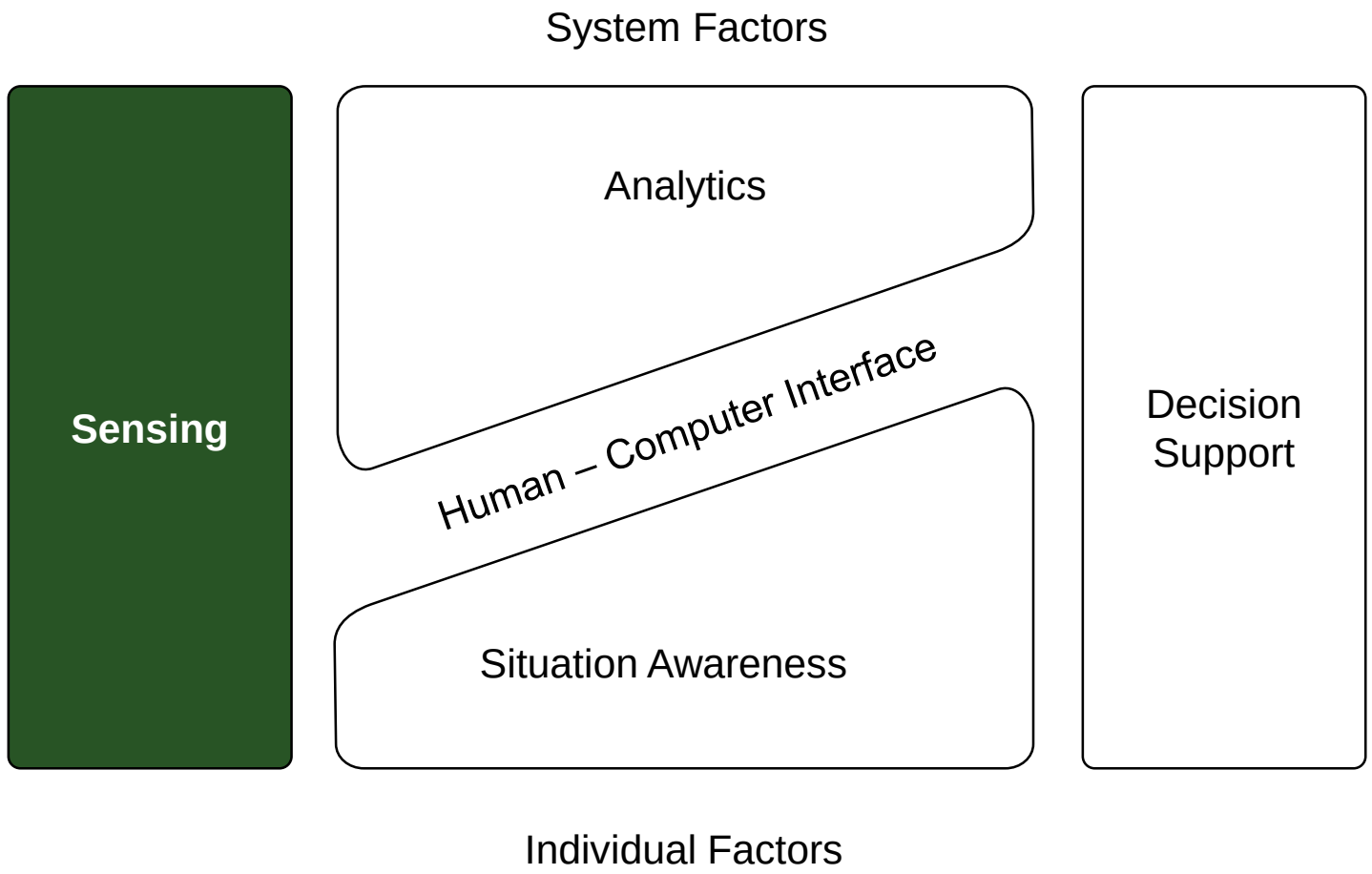


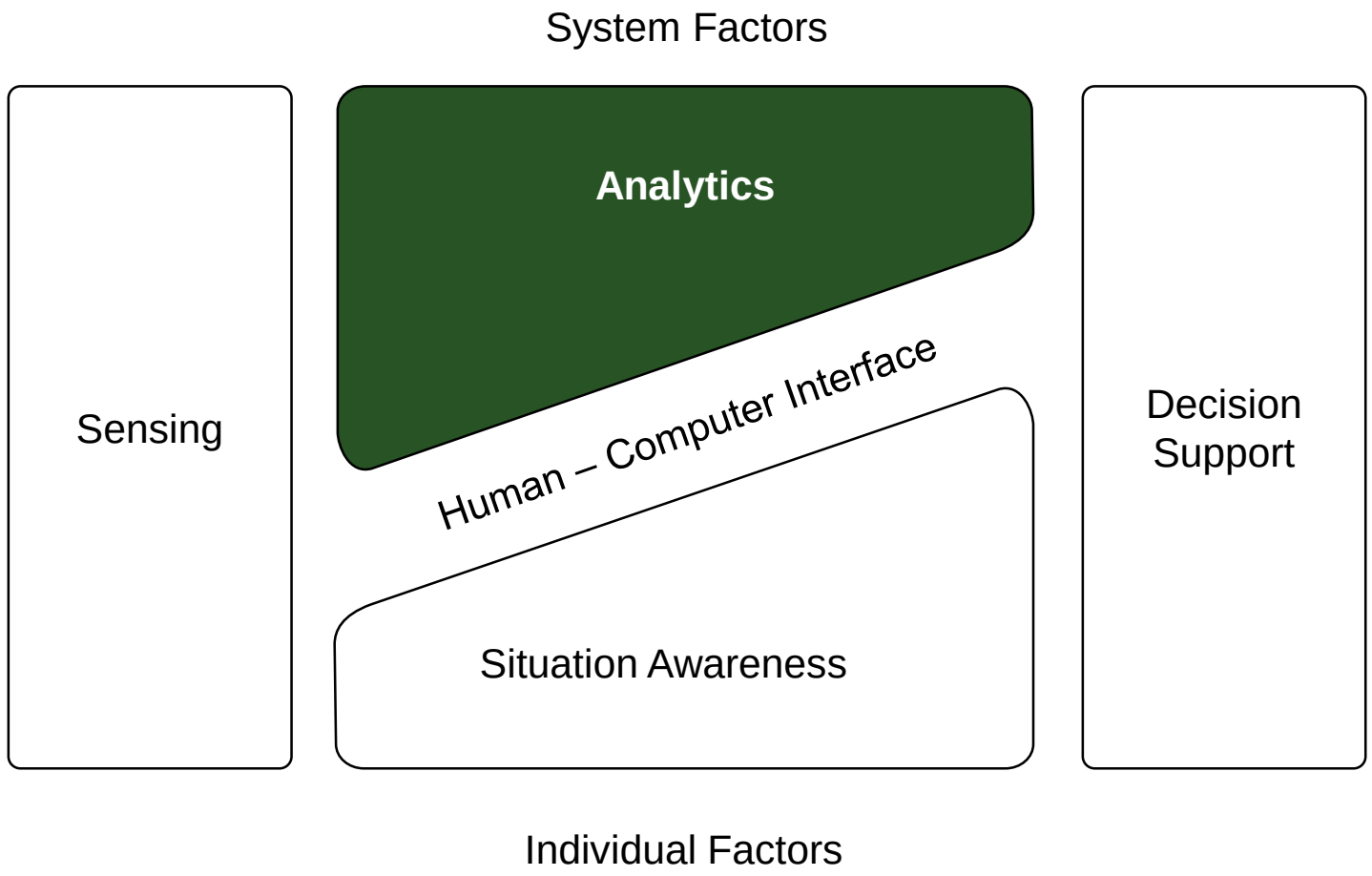


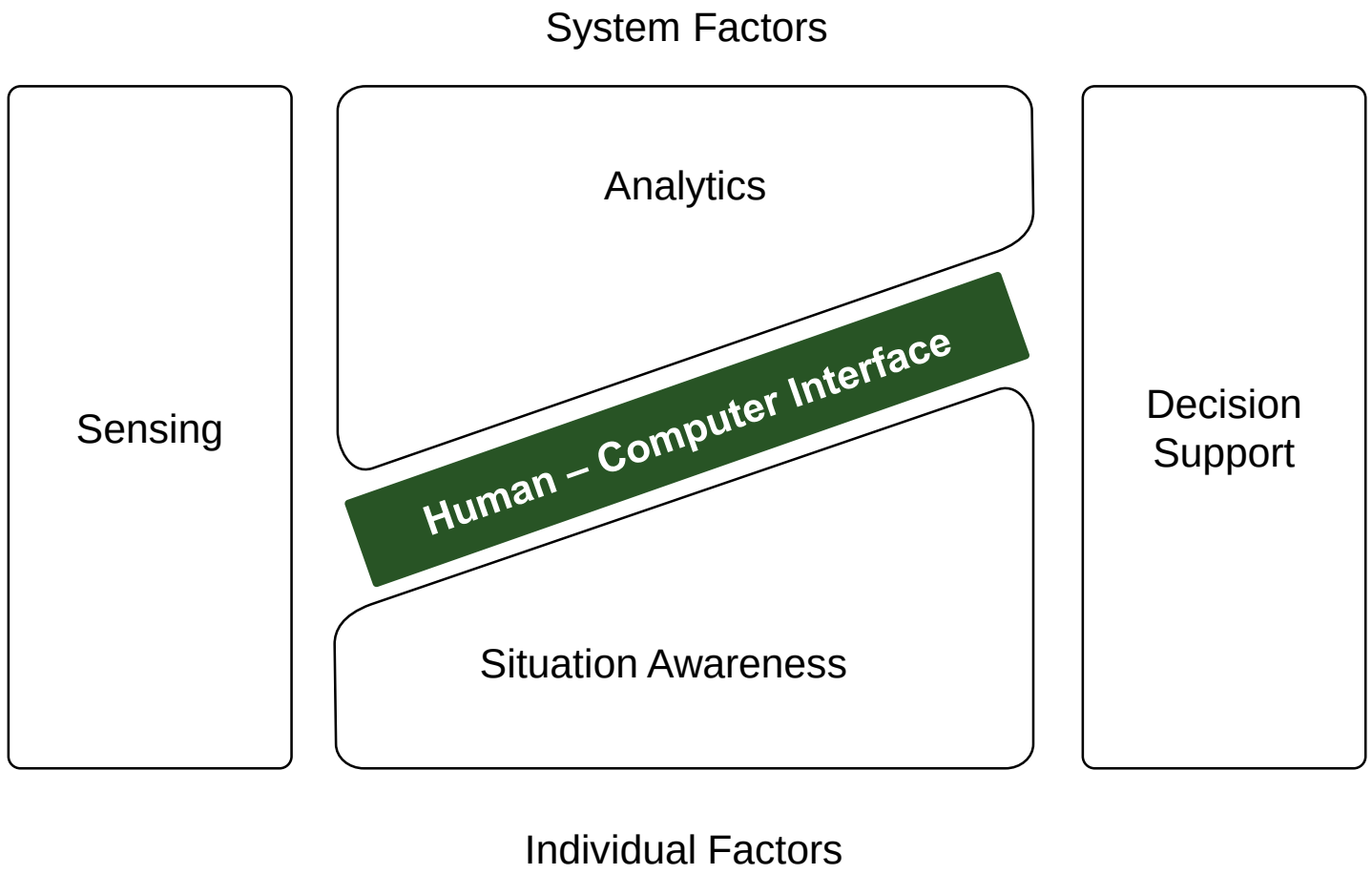
Polling Question 3:

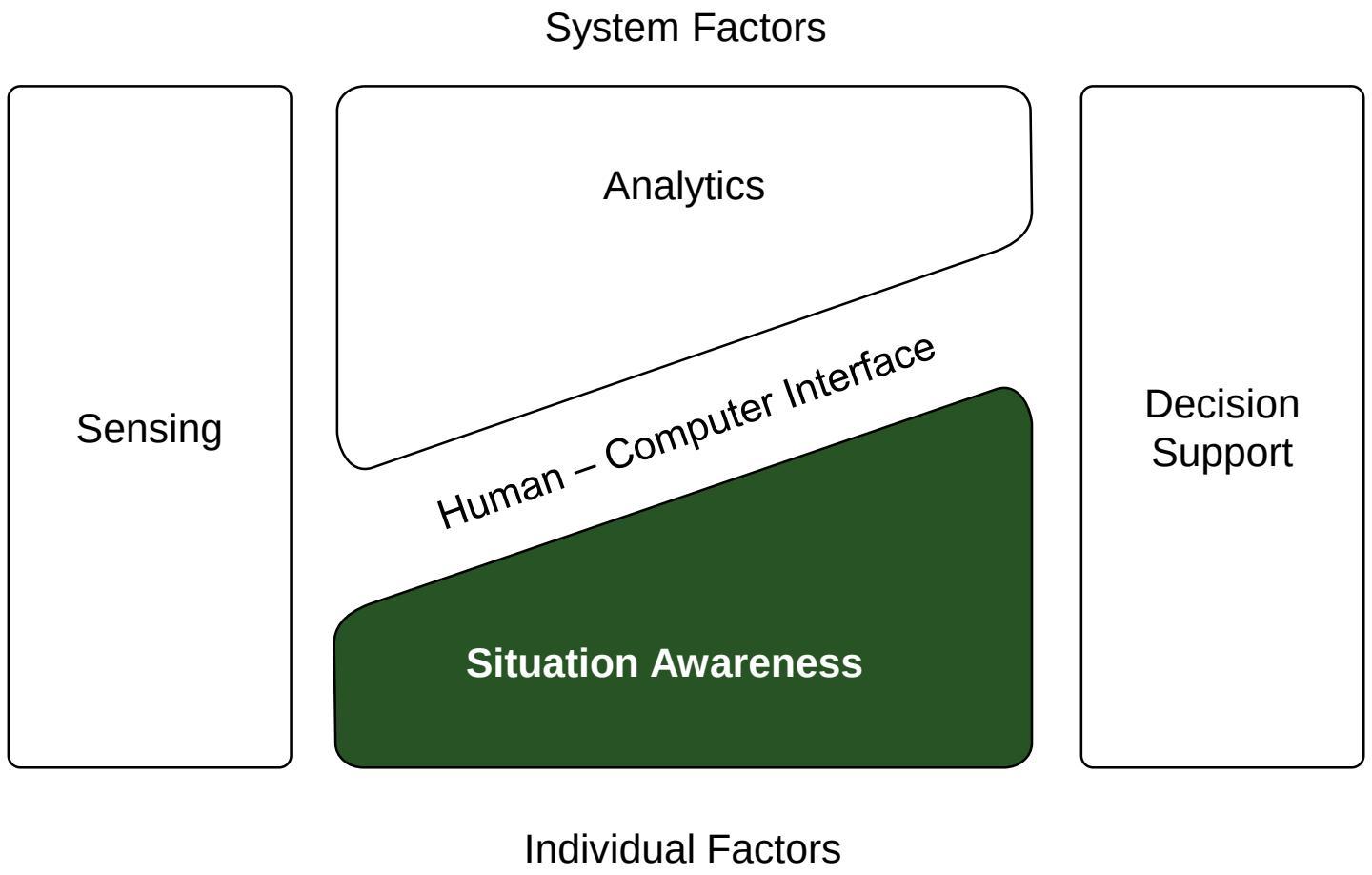
What should we discuss in more detail?

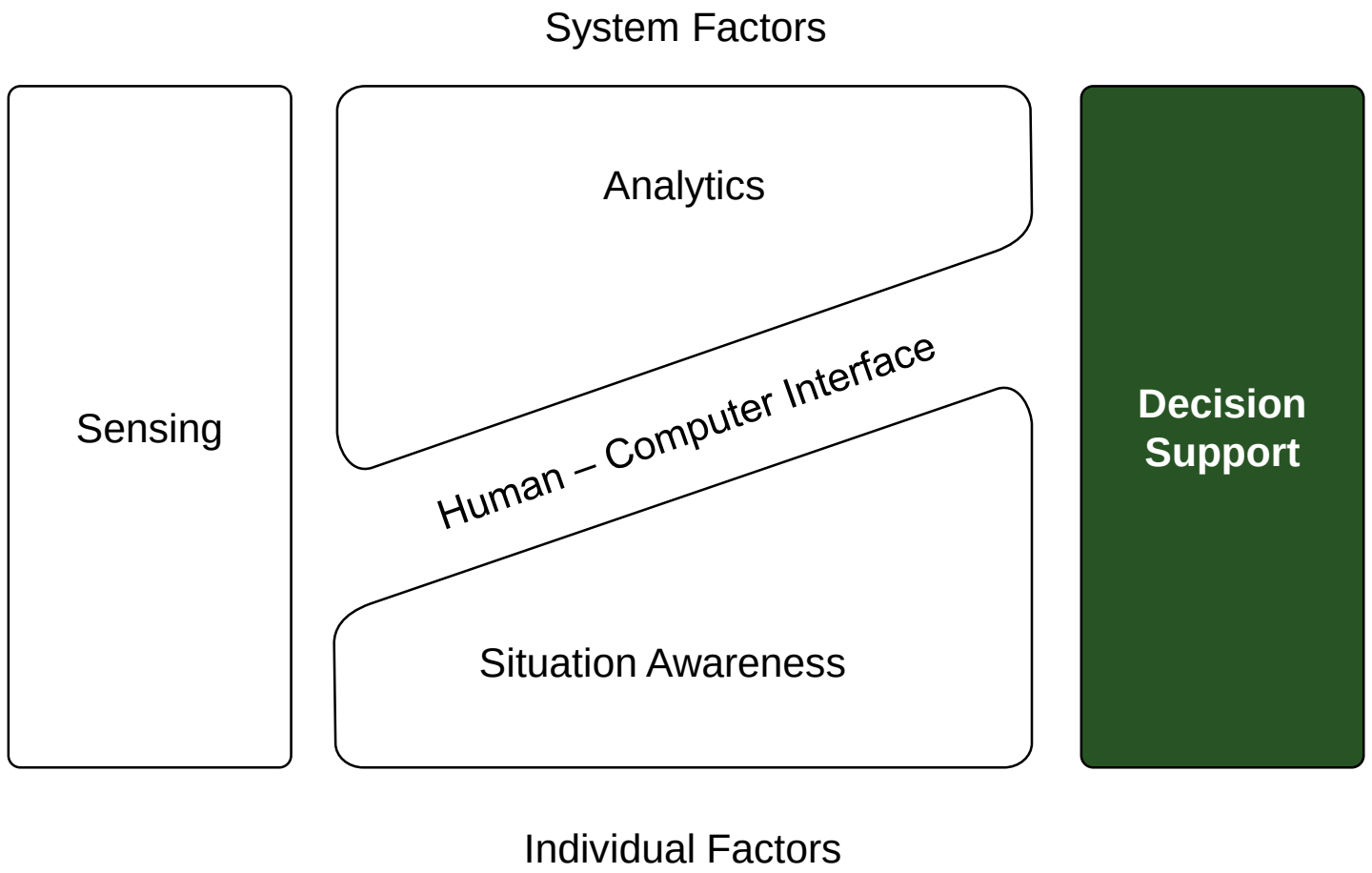












12th Annual Open Forum
for Large-Scale Network Analytics